ガロア体の整数基について (P進L関数と代数体の整数論)

AUTHOR(S):

黒田, 成信

CITATION:

黒田, 成信. ガロア体の整数基について (P進L関数と代数体の整数論). 数理解析研究所講究録 1981, 411: 170-175

ISSUE DATE:

1981-01

URL:

http://hdl.handle.net/2433/102412

数理解析研究所講究録
411巻 1981年 170-175

ガロア体の整数基について

東大 教養 黒田 成信

§0. A を Dedekind 環, K をその商体とし, L/K は有限次の分離的拡大体とし, $n=[L:K]$ とおく. B を L に於ける A の整閉とする. そのとき B は Dedekind 環であり, A-加群として, n-個の A-ideal の直和と同型である. もし B の n 個の元 ω_ν $(1\leq\nu\leq n)$ が存在し

$$B = A\omega_1 + A\omega_2 + \cdots + A\omega_n$$

となるとき, L/K は整数基をもつということにしよう. このとき, 上の和は直和となる.

$L=K(\theta)$ とし, θ の L/K に関する判別式を $d(\theta)$, B/A の判別式を $\mathfrak{d}(L/K)$ で表わそう. そのとき $\mathfrak{d}(L/K)=d(\theta)\cdot\mathfrak{a}^{-2}$ となる. ここで, $\theta\in B$ に取ってあれば, $\mathfrak{a}$ は A-ideal である.

§1. 記号は上記の通りとする. Artin [1] によれば次が成立する:

L/K が整数基をもつ $\Longleftrightarrow$ $\mathfrak{a}$ は A の principal ideal.

この必要十分条件は少しく変形すれば次のようになる：

$$L/K \text{ が整数基をもつ} \Longleftrightarrow \exists \delta \in A,\ \mathfrak{d}(L/K)=(\delta) \text{ かつ } K(\sqrt{d(\theta)}) = K(\sqrt{\delta}).$$

しかし，体の拡大 L/K は必ずしも初めから生成元 θ により $L=K(\theta)$ の形に与えられているものとも限らない、例えば，あるAbel体が類体として定義されている場合である、以下に於て我々は L/K が Galois 拡大のときに限ることにより，L/K が整数基をもつための必要十分条件を，生成元 θ に関係しない形で与える、更に，それを後に引用する Fröhlich による判定条件と比較することにより，定式化に於て整数基の存否と関係しない算術的命題を得る(定理3)、

§2、有限群 G の位数を割る最小の素数を p とする．もし G の p-Sylow 群 S が巡回群であれば，G の元で位数が p と素なもの全体は G の正規部分群 N をなし，G は N の S による半直積となる(Burnside)．従って Galois 拡大 L/K の Galois 群の 2-Sylow 群が巡回群で単位群とは異なるとき，L/K は丁度一

つの次数2の部分体を含むこととなる.

我々の考察に於て, Kの標数が2のときの方が, そうでないときより結果は簡単になるので, 以下Kの標数は2でないとし, この仮定を繰返して述べることは省略する.

定理1. L/K はGalois拡大とし, S をそのGalois群の2-Sylow群とする.

Ⅰ. $S = E$ = 単位群のとき:

L/K が整数基をもつ $\Longleftrightarrow \exists \delta \in A$, $\mathfrak{d}(L/K) = (\delta^2)$.

Ⅱ. S 巡回群, $\neq E$ のとき:

L/K が整数基をもつ $\Longleftrightarrow \exists \delta \in A$, $\mathfrak{d}(L/K) = (\delta)$ かつ

$K(\sqrt{\delta})/K$ は L/K に含まれる

次数2の拡大となる.

Ⅲ. S 非巡回群のとき:

L/K が整数基をもつ $\Longleftrightarrow \exists \delta \in A$, $\mathfrak{d}(L/K) = (\delta^2)$.

後での引用の便宜上次の系を定式化する.

系. L/K は2べき次の巡回拡大で, A の素イデアルはすべて L/K で不分岐とする. そのとき次が成立する.

L/K が整数基をもつ $\Longleftrightarrow \exists \varepsilon$ A の単数, $L \supset K(\sqrt{\varepsilon}) \supsetneq K$.

上の定理に於て L/K の次数が2のときは，Mann [6] の判定条件である．

定理1を証明するには，$L=K(\theta)$，$\tilde{\theta}^{(\nu)}=(1,\ \theta^{\sigma_\nu},\ \cdots,\ (\theta^{n-1})^{\sigma_\nu})$，$\sigma_\nu\in Gal(L/K)$ とおくとき，$Gal(L/K)$ が集合

$$\{\tilde{\theta}^{(1)},\ \tilde{\theta}^{(2)},\ \cdots\cdots,\ \tilde{\theta}^{(n)}\},\qquad n=[L:K],$$

の上の transitive regular permutation group であることと，$d(\theta)$ の定義および $\{\operatorname{sgn}\sigma\mid\sigma\in Gal(L/K)\}$ が定理の中の I. II. III. に対応してそれぞれ $\{1\}$, $\{\pm1\}$, $\{1\}$ であることに注意して，§1の判定条件に帰着させるのである．

§3. 以下 K は有限次代数体，A は K の全整数環とする（K が有限体を定数体とする一変数代数函数体の場合でもよい）．K のイデール群，主イデール群，準イデール群をそれぞれ J_K，P_K，U_K で表わす．次数有限の拡大体 L/K のイデール論的判別式（局所的判別式の積）を今仮に $\bar{\mathfrak{d}}(L/K)$ で表わす．$\bar{\mathfrak{d}}(L/K)$ は $\bmod. U_K^2$ で定まり $P_KJ_K^2$ に属する．$\bar{\mathfrak{d}}(L/K)$ に対応するイデアルはもちろん $\mathfrak{d}(L/K)$ で，又，イデアル論的判別式の場合と同じ形の連鎖律などが成立する．さて

$$L/K\text{ が整数基をもつ}\iff\bar{\mathfrak{d}}(L/K)\in P_KU_K^2$$

が成立する．以上は Fröhlich [3], [4], [5] などよりの部分的引用である．

§4. K は §3 の通りとし，以下次の仮定と記号を設定する．

L/K: Kのすべての素点で不分岐な2べき次の巡回拡大，$[L:K]=2^m$.

$L=K_m \supset K_{m-1} \supset \cdots \supset K_0=K$, $[K_\mu : K_0]=2^\mu$.

§2 の系によれば，K_m/K_0 が整数基をもつことと，K_1/K_0 が整数基をもつことは同値であるが，今上の仮定のもとで次が成立する．

定理2. K_m/K_0 が整数基をもつ $\iff$ $\forall \mu, \mu'$, $m \geq \mu \geq \mu' \geq 0$, $K_\mu/K_{\mu'}$ が整数基をもつ．

証明は，$P_K J_K^2 \cap P_K U_K = P_K U_K^2$ や L/K の不分岐性などを利用して，§3 で引用した Fröhlich の判定条件に帰着させるのである．(Hasse のノルム定理や，上のような $K_\mu/K_{\mu'}$ では $K_{\mu'}$ の単数は K_μ の数のノルムとなることなどを使う)．

再び，§2 の系を用いて，次を得る．

定理3. $\exists \varepsilon_0$, K_0 の単数, $K_1 = K_0(\sqrt{\varepsilon_0})$

$\Longleftrightarrow$ $\forall \mu$, $m > \mu \geq 0$, $\exists \varepsilon_\mu$, K_μ の単数, $K_{\mu+1} = K_\mu(\sqrt{\varepsilon_\mu})$.

K_0 が1の原始4乗根を含むときには，定理3の主張は文献 Cohn and Cooke [2] の中にある．そこでは Kummer 論と類体論の両方を使って証明している．

文献

[1] E. Artin, Question de base minimale dans la théorie des nombres algébriques, 全集 229-231.

[2] H. Cohn and Cooke, G., Parametric form of an eight class field, Acta Arith., 30(1976), 367-377.

[3] A. Fröhlich, Discriminants of algebraic number fields, Math. Zeitschr. 74(1960), 18-28.

[4] ———, Ideals in an extension field ···, Math. Zeitschr. 74 (1960), 29-38.

[5] ———, The discriminants of relative extensions and the existence of integral basis, Mathematika 7(1960), 15-22.

[6] H.B. Mann, On integral bases, Proc. Amer. Math. Soc., 9(1958), 167-173.